NETSCAPE SECURITY

A Working Note
For NAVSUP Claimancy

9 April 2001

NETSCAPE SECURITY

INTRODUCTION

The Department of Defense (DoD) has been developing a strategy to provide information assurance within the Defense Information Infrastructure (DII). One of the significant developments in deploying this strategy was the completion of a purchase of FIPS compliant browser and server products from the Netscape Communications Corporation. This contract was procured by the Defense Information Systems Agency (DISA) under the Integrated Computer-Aided Software Engineering (I-CASE) contract. It was renewed on March 27, 2001. Included in the renewal is the iPlanet Portal Server software for up to 300 central processing units and as many as 2 million users. DoD plans to deploy the iPlanet Portal Server to introduce a new Web portal, designed initially for internal employee use and in the future to serve suppliers and other external vendors and citizens working with DoD.

Included in the contract is the Netscape Communicator Client (professional edition). The modules of the Communicator Client are as follows:

Netscape Navigator - Access information using the world's leading client for browsing and hosting applications.

Netscape Messenger - Compose, send, and receive encrypted email with the full richness of the Web using open standards-based mail.

Netscape Collabra – Collaborate with coworkers and leverage corporate knowledge more easily and effectively.

Netscape Composer - Create and publish richly formatted HTML documents with ease.

Netscape Netcaster – Experience dynamic, personalized information pushed to you through the best channels on the Web.

Netscape Conference - Communicate with coworkers using real-time voice and information collaboration.

Netscape AOL Instant Messenger - Instantly exchange messages with friends, family, and colleagues.

Netscape Calendar – Manage your calendar and time with coworkers.

Netscape AutoAdmin – Allows Netscape Communicator to be centrally managed.

Netscape IBM Host On-Demand - Access IBM host information.

The contract also includes the following server licenses to support the Communicator capabilities:

iPlanet Web Server Enterprise Edition 4.1 [formerly: Enterprise Server] - A security-enhanced web server for creating, managing and distributing information, and running intranet and Internet applications

FAST TRACK - has been updated with iPlanet™ Web Server, FastTrack Edition 4.1: The first free Web server with integrated SSL, LDAP and Java™technology support.

iPlanet Portal Server - The iPlanet™ Portal Services platform creates portals for an organization's integrated data, knowledge management and applications.

Messaging Server - An open standards-based client-server messaging system that provides administration, scalability, performance, security, and remote connectivity.

Collabra Server - An open standards-based server that facilitates collaboration by letting organizations create, publish, and maintain private and public discussion groups.

iPlanet Directory Server - A directory server based on the Lightweight Directory Access Protocol (LDAP).

iPlanet Certificate Management System - Server software that enables DOD organizations to issue, sign, and manage public-key certificates using the Secure Sockets Layer (SSL) protocol for encrypted, private communication over a corporate intranet or the Internet.

Mission Control - With Mission Control, IT professionals can customize Netscape Communicator's user interface, and create customized installations of Communicator.

Security Services - Netscape Security Services (NSS) is a complete security infrastructure that will allow organizations to deploy a wide variety of applications that can utilize the cryptography services provided by NSS on Client and Server platforms.

This license was acquired to support security and interoperability for the DoD as a whole. Establishing a single Internet suite is expected to lower training costs and assure deployment of applications and tools that run across all vendors' hardware, operating systems, and databases. NIST's validation of Netscape's conformance to the FIPS 140-1 standard ensures that the Government users are in compliance with the mandated standard for secure software cryptography. A higher degree of assurance is also possible with the availability of the FORTEZZA versions of the products.

Additional information on the Netscape products available under this DoD license is available at http://dii-sw.ncr.disa.mil/Del/netlic.html.

PUBLIC KEY INFRASTRUCTURE: The Navy Acquisition PKI (NA PKI) is a pilot project that established a Public Key Infrastructure (PKI) within the Naval Supply Systems Command. NAVSUP is now in the process of migrating from this pilot project to the Department of Defense Public Key Infrastructure (DoD PKI). Both the NA PKI and the DoD PKI use the Netscape suite to implement the infrastructure. The purpose of this working note is not to discuss the security aspects of the entire Netscape suite, but rather, to concentrate on the browser, Navigator.

NETSCAPE NAVIGATOR

Netscape Navigator is the browser available with the Communicator suite. Security features of the browser can be divided into two basic categories. First are those configuration settings (preferences) that allow the user to decide upon the protection features to be enabled. Second are the features that allow encrypted transmission between client and server.

BROWSER PREFERENCE SETTINGS

To access the browser settings, select Edit from the menu bar and then select Preferences from the drop-down menu. In the dialog box that appears, the window on the left side will show the categories of options in a directory-like tree structure. To the right of the categories window is an explanation of the selected category, together with options for that category. Browser features addressing security issues are viewed by selecting Advanced.

By default, all six options are checked. If a browser user is unwilling to trust Java applets to run automatically or allow JavaScript code embedded in an HTML page to execute, those options may be turned off. The recommendation is to allow both Java options as long as you can reasonably trust the web server you are communicating with. If you aren't sure, turn them off for the browsing session and reset them later. Many applications using browser clients require that Java be enabled. If you must do business with those sites, you will need to enable Java.

At the bottom of the right side of the window are the Cookies options. By default, the browser is configured to accept all cookies. However, the browser user has the option of accepting only cookies that get sent back to the originating server, disabling cookies transmission, or receiving a notification dialog box when Communicator accepts a cookie. The topic of cookies is covered in a separate working note. Using the browser for official business, you should be comfortable with the setting that accepts only those that get sent back to the originating server.

The next security feature allows the browser to make use of firewall proxies to securely handle browser requests. Click on the '+' to the left of the Advanced category. This expands the Advanced features to show Cache, Proxies, and Disk Space. Select

Proxies to display the options in the right half of the window. If your site has a firewall in place, select Manual Proxy Configuration and click on View. Enter the name of your firewall in the space available for HTTP, Security, Gopher, and WAIS. For each entry, the port number is 80. Click OK for the Manual Proxy Configuration and then OK for the Preferences dialog.

This completes the Preferences settings that control how the browser works. Next we will address the secure communications features of Netscape Communicator.

BROWSER SECURITY SETTINGS

To access security settings, you may either click on the Security icon on the Navigation Toolbar (if it isn't visible, select View on the menu toolbar and then Show Navigation Toolbar on the drop-down menu), or on the menu bar select Communicator, Tools, and then Security Info on the drop-down menu. Netscape will start in a new window and display a scrolling window on the left with Security Info highlighted. The title Security Info displays at the top left and on the right is information about the encryption and verification available for the page currently loaded in Navigator. You will be informed whether or not the page was encrypted and some notes on site verification. You can view all details of the displayed page by clicking on Open Page Info.

The next option is Passwords. Click on Passwords option in the scrolling window to display the panel to set or change your password. This password is set for your Communicator software only and is especially important if you have digital certificates installed in Communicator. Three options are presented for password prompting. Choose the third option and set the time out for 30 minutes or less. This will allow you to enter your password one time and use it as often as needed. After 30 minutes of inactivity, you will be prompted again for your password the next time it is required.

Selecting Navigator option displays choices for your notification should you attempt to do something that might be unsafe.

1. Entering an encrypted site: You need to be aware that the pages you are accessing are encrypted. Because the pages are decrypted without your intervention, you may want notification to remind you that you must clean up or secure downloaded files upon completion of your session.
2. Leaving an encrypted site: You may want this as a reminder when to remove decrypted files left on your local drive. Web pages are only encrypted during transmission from the web page server to your browser. Files in your cache or file you may have saved to disk are not encrypted.
3. Viewing a page with an encrypted/non encrypted mix: You may want this as a reminder to consult the Security Info panel, which identifies files encrypted during transmission.
4. Sending non encrypted information to a site: You may want this as a reminder to help to prevent you from submitting non encrypted forms or information that you may not realize is submitted through email.

The next section is labeled “Certificate to identify you to a web site.” A certificate, if you have one, includes your digital signature. If you have multiple certificates of your own, you can choose which you want to send to a web server. Some web sites may only accept certificates from specific signers or certificates exceeding a particular grade. The easiest means of selecting which certificate to use is to use the setting to Select Automatically. If you frequently transact with multiple sites that have conflicting requirements, set Ask Every Time.

The last section on this panel shows, by default, that your browser is configured to enable both versions 2 and 3 of Secure Sockets Layer (SSL). These should not be changed. SSL provides an encrypted link between a browser and a secure web server. If SSL is disabled on the browser, it cannot be linked to a secured web server.

The next option in the scroll panel is Messenger. If you installed only the standalone Netscape Navigator instead of Communicator, this option will not be available on your menu. Because NAVSUP chose Lotus Notes as its messaging system, we will not be concerned with Messenger settings. You can find out about these features by selecting Help at the bottom of this window.

Java/JavaScript is the next option. Software developers can sign their work with digital certificates. When you accept signed modules, the certificates will be placed in this area. Use the Java Applets panel to view, remove, and edit access privileges for Java applets signed with a certificate issued by the signer listed in the list box. This gives the user control over whose Java applets and scripts will be accepted and their level of access.

The next option is Certificates. A certificate is a file that identifies a person, a server, or organization. Communicator uses certificates to encrypt information. You can use a certificate to check the identity of the certificate's owner. You should trust a certificate only if you trust the person or organization that issued it. Your own certificates allow you to receive encrypted information. Communicator also keeps track of certificates from other people, web sites, applets, and scripts. Numerous authorities issue certificates. These Certificate Authorities (CAs) can be government, private, or commercial. One of the best-known commercial CAs is VeriSign, Inc.

When you apply for and receive a certificate using the Communicator browser, such as a Navy Acquisition or DoD PKI certificate, it will appear under “Yours.” You also have the ability to import a certificate exported to a file from another software package. A single user may have several certificates.

The “People” selection will show those certificates that belong to the people you communicate with. Whenever a signed email is received with Communicator, the sender’s certificate is placed in this area. You can also search for user certificates in a

directory. These certificates may be used to encrypt outgoing email from Communicator. (This feature will not be used in the NAVSUP Lotus Notes environment.)

Secure servers also deliver digital certificates when an SSL session is being established with your browser. If a certificate you receive is not from a Certificate Authority (CA) recognized by your browser, you will be prompted to trust it manually. When you trust such a certificate it is placed in the Web Sites area. For server certificates signed by recognized CAs you will not be prompted, and the browser will implicitly trust the certificate. Those certificates are not added to this list.

Signer certificates are those that identify Certificate Authorities, or signers of certificates for servers and users. Communicator comes with a list of common signers already installed. As you interact with a CA that is not in this list, you will be prompted to manually accept the CA certificate. It will then be added to this list. This will be the case with both the NA PKI and the DoD PKI. When you apply for a digital certificate you will be prompted to accept the CA certificate.

Cryptographic Modules completes the options list. These are loadable pieces of software that provide a function of cryptographic services, such as: smart card support (including PCMCIA smart cards and disk-based smart cards); specialized key distribution schemes, such as Entrust; hardware-accelerated cryptography (currently unavailable); new ciphers (currently unavailable); and FIPS-compliancy. By default Communicator installs with its own internal module called PKCS#11.

MULTI-USER BROWSER ENVIRONMENT

Communicator provides the capability to administer user profiles. This allows one software installation to serve multiple users, each with his/her own preferences and security attributes. This feature may become more important in the near future as web-enabled applications are developed that require individual user authentication implemented through digital certificates.

Upon installation of Communicator, the setup process includes several panels for establishing a user profile. Most likely, in single-user-per-workstation environments, this information is not established and the installation proceeds using default information. After installation, this default information may be edited and additional user profiles created using the User Profile Manager.

The User Profile Manager is run by selecting Start, Programs, Netscape Communicator, Utilities, User Profile Manager. The Manager opens a window in which appears the list of known user profiles. Manager allows the editing, addition and deletion of these profiles. When two or more profiles exist, Communicator will now start with this user profile selection window. The user chooses the profile needed for the session and then selects Start Communicator to initiate the Communicator session. At that point,

the associated user file loads the preference and security information associated with that profile.

This is an important point, because there is no password on the use of any profile. However, as explained earlier, there is a Communicator password that provides protection for the certificates in that profile. This is the feature that provides protection for an individual user. Because the certificates are the means by which a user is identified and authenticated to web servers, the ability to secure them is a necessity.

SUMMARY

A number of features of the Netscape Navigator browser provide the individual user the means to configure browser features to match personal preferences. These include the acceptance or refusal of Java, JavaScript, and cookies features of web communication. A security profile, including the use of digital certificates for identification and authentication of the user to certain web servers, provides for personal privacy. A password is used to prevent anyone else from using your private digital certificates. Finally, Communicator itself provides the capability to create multiple user profiles, making it possible for several users to share a single browser installation on one machine, yet retain personal browser configuration preferences and maintain privacy for personal digital certificates.

HOW TO OBTAIN NETSCAPE COMMUNICATOR

A DISA contractor maintains a download site that is available to Department of Defense employees and contractors. The URL for the site is http://netscape.intdec.com/disa/. Your browser should be set to accept cookies and you must be working from a ".mil" IP address. On your first visit to the download site, you must register as a user. On subsequent visits, you must authenticate yourself to the site in order to download files

The DISA license site provides the following guidelines: "Authorized users may download one (1) copy of a Netscape product Client/Server and redistribute it to other authorized users within their organization. However, you must send an email message to reinharr@ncr.disa.mil that includes information about the product(s) downloaded and the number of people using each product [e.g. "one copy of iPlanet Directory Server downloaded - 50 users"; we do not need the names of the individuals using the software]. This data is in addition to the information provided during the download procedures. The message should also include a brief project description, and the name, organization, and telephone number (commercial and DSN) of the individual who has been designated as the POC for the redistributed products."

DoD employees may also use this software on their home systems. To verify this, visit the Netscape DoD License homepage at http://dii-sw.ncr.disa.mil/Del/netlic.html and read paragraph 3, covered users.

After installation, run Navigator and select Help, About Communicator. Scroll down to the section on RSA. The second paragraph should contain the following: “This version supports U.S. security with RSA Public Key Cryptography…”. If this statement is not present, you are using the export version with weaker encryption keys. You should be using the version for US and Canada that provides for stronger encryption using a 128-bit key.